IN THE CLAIMS:

Please amend claims 1-3, 6, 9-15, 18, 19, 21, 24, and 25 as shown in this complete set of all pending claims:

1. (Currently Amended) A data processing unit for executing an encrypted ~~software~~ executable program, the data processing unit comprising:
   a processor for decrypting the encrypted ~~software~~ executable program and for executing the ~~software~~ executable program, the processor including an identifying number, the identifying number being accessible only by the processor; and
   a memory unit, the memory unit storing the decryption procedure, the encrypted executable program being encrypted using at least a portion of the identifying number;
   wherein, when the processor is to execute the ~~software~~ executable program, the ~~software~~ executable program is decrypted using the decryption procedure along with the identifying number.

2. (Currently Amended) The data processing unit as recited in claim 1 wherein the encrypted ~~software~~ executable program is stored in the memory unit.

3. (Currently Amended) The data processing unit as recited in claim 1 further comprising an external memory unit, wherein the encrypted ~~software~~ executable program is stored in an external memory unit.

4. (Original) The data processing unit as recited in claim 1 wherein the identifying number is a serial number.

5. (Original) The data processing unit as recited in claim 1 wherein the identifying number is associated with a plurality of data processing units.

6. (Currently Amended) A method for protecting ~~software~~ executable programs, the method comprising:

providing a data processing unit with an identifying number, the identifying number being accessible only by the processing unit;

encrypting ~~a software~~ an executable program external to the data processing unit using at least a portion of the identifying number; and

decrypting the encrypted ~~software~~ executable program prior to execution of the ~~software~~ executable program by the data processing unit using the identifying number and a decryption procedure stored in the data processing unit.

7. (Cancelled)

8. (Previously Presented) The method as recited in claim 6 wherein the identifying number is a serial number for the data processing unit.

9. (Currently Amended) The method as recited in claim 6 wherein the encrypted ~~software~~ executable program is stored external to the data processing unit.

10. (Currently Amended) The method as recited in claim 6 wherein the encrypted executable program is stored in the data processing unit.

11. (Currently Amended) A data processing system, the system comprising:

a host data processing unit, ~~the data processing unit including an identifying number stored therein, the identifying number being accessible only by the data processing unit,~~ the host processing unit encrypting ~~a software~~ an executable program using at least a portion of ~~the~~ an identifying number; and

a target data processing unit, the target data processing unit decrypting the ~~software~~ executable program[[s]] with a software procedure using a decryption key based on the identifying number~~;~~

~~wherein the data processing unit decodes an encrypted software program applied thereto using the decryption key~~.

12. (Currently Amended) The system as recited in claim 11 wherein the identifying number is a serial number for the target data processing unit.

13. (Currently Amended) The system as recited in claim 11 further comprising a memory unit external to the target data processing unit, the memory unit storing encrypted ~~software~~ executable programs.

14. (Currently Amended) The system as recited in claim 11 further comprising a memory unit in the target data processing unit, the memory unit storing encrypted ~~software~~ executable programs prior to decryption.

15. (Currently Amended) The system as recited in claim 11 wherein an encrypted program is decrypted as an entity or on the fly prior to execution of the ~~software~~ executable program by the target data processing unit.

16. (Cancelled)

17. (Cancelled)

18. (Currently Amended) The system as recited in claim 15 wherein decrypted portions of the ~~software~~ executable program are stored in a protected memory unit accessible to only the target data processing unit.

19. (Currently Amended) A method for protecting an execution of ~~a software~~ an executable file, the method comprising:

providing a target processor with an identifying/serial number accessible only to the target processor;

encrypting the ~~software~~ executable file using at least a portion of the identifying/serial number;

applying the encrypted ~~software~~ executable file to the target processor; and

decrypting the encrypted ~~software~~ executable file using a decryption procedure stored in the target processor and the identifying/serial number.

20. (Cancelled)

21. (Currently Amended) An apparatus for secure transfer of ~~software~~ executable files, the apparatus comprising:

a first processor, the first processor having a program for encrypting ~~a software~~ an executable file using an identifying/serial number; and

a second processor, the second processor having a decryption procedure stored in a memory coupled to the second processor for decrypting the ~~software~~ executable file[[s]] using at least a portion of ~~an~~ the identifying/serial number stored in the second processor, the stored identifying/serial number being accessible only to the second processor.

22. (Cancelled)

23. (Previously Presented) The apparatus as recited in claim 21 wherein the at least a portion of the identifying/serial number is accessed by the first processor based on an indicia of the second processor.

24. (Currently Amended) The apparatus as recited in claim 21 wherein an encrypted ~~software~~ executable file is stored in an unsecured storage unit.

25. (Currently Amended) The apparatus as recited in claim 24 wherein the encrypted ~~software~~ executable file is stored in [[an]] the unsecured storage unit prior to decryption.